

UNITED STATES DISTRICT COURT **FILED**
for the
Southern District of Ohio
AUG 8 2019

Richard W. Nagel
Clerk of Court, Dayton OH

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

1216 Cloverfield Avenue Apartment D, Kettering, Ohio.

Case No.

3:19-mj-477

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. § 922(g)(3)
18 U.S.C. § 922(a)(6)
18 U.S.C. § 924(a)(1)(A)
18 U.S.C. § 1001
21 U.S.C. § 844

Offense Description
Possession of a firearm/ammunition by an unlawful user of a controlled substance
or by a person addicted to a controlled substance
false statement regarding firearms
false statement regarding firearms
false statement
unlawful possession of a controlled substance

The application is based on these facts:

See Attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

Date: 08/08/2019

City and state: Dayton, Ohio

Applicant's signature

SA P. Andrew Gagan, FBI

Printed name and title

Judge's signature

Hon. Michael J. Newman U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

Property to be searched

The property to be searched is **1216 Cloverfield Avenue, Apartment D, Kettering, Ohio 45429**, further described as an apartment rented by **Ethan KOLLIE** and located at 1216 Cloverfield Avenue, Kettering, Ohio 45429, within a large multi-unit brick building with multiple front facing windows and blue shutters, as depicted in the photograph below. The apartment building has four tan in color pillars on the front of the building. The building has a concrete walkway leading from the sidewalk to a small concrete porch located near the front door. The front door is a large tan door with five small windows on each side. The apartment building's landscape consists of multiple small bushes running across the front of the building and two medium sized trees in the front yard. The building has a concrete driveway on the left side of the home leading to a large multiple car garage.



ATTACHMENT B

Property to be seized

1. All records relating to violations of:

- 18 U.S.C. § 922(g)(3)
- 18 U.S.C. § 922(a)(6)
- 18 U.S.C. § 924(a)(1)(A)
- 18 U.S.C. § 1001
- 21 U.S.C. § 844

involving **Ethan KOLLIE** and occurring after **2013**, including:

- a. any information related to the purchase, use, or possession of firearms;
- b. any information related to the purchase, use, or sale of controlled substances;
- c. any information related to the types, amounts, and prices of controlled substances or firearms purchased, used, or trafficked as well as dates, places, and amounts of specific transactions;
- d. any information related to sources of controlled substances or firearms (including names, addresses, phone numbers, or any other identifying information);
- e. any information recording **KOLLIE's** schedule or travel from 2013 to the present;
- f. all bank records, checks, credit card bills, account information, and other financial records.

- g. records of Internet Protocol addresses used;
 - h. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
2. Computers or storage media used as a means to commit the violations described above.
3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):
- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;

- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite"

web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

- m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law

enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF THE
PREMISES OF 1216 CLOVERFIELD
AVENUE APARTMENT D, KETTERING,
OHIO

Case No. 3:19-mj-477

AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE

I, P. Andrew Gagan, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as **1216 Cloverfield Avenue Apartment D, Kettering, Ohio**, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), Cincinnati Division. I have been employed as a Special Agent with the FBI since May 2016. I have received training in national-security investigations and criminal investigations, and I have conducted investigations related to international terrorism, white-collar crimes, drug trafficking, public corruption, and violent crimes. As part of these investigations, I have participated in physical surveillance and records analysis, worked with informants, conducted interviews, served court orders and subpoenas, and executed search warrants.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

4. On or about August 4, 2019, agents with the FBI and ATF (Bureau of Alcohol, Tobacco, Firearms and Explosives) interviewed **Ethan KOLLIE (KOLLIE)**, at the PREMISES, in connection with the mass shooting earlier that day in Dayton, Ohio, committed by **Conner Stephen BETTS (BETTS)**. **KOLLIE** indicated that he liked guns and currently owns a handgun and a micro Draco pistol. He also indicated that he purchased body armor and a firearm accessory for **BETTS** earlier this year. **KOLLIE** consented to a search of his residence. While inside, the agents smelled marijuana and observed, in plain sight, paraphernalia consistent with smoking marijuana including, what appeared to be commonly referred to as a “bong,” which is a drug delivery device commonly used to smoke marijuana. Agents also observed in plain sight, on the counter, what they believed to be the Draco pistol. **KOLLIE** indicated that his handgun was in his bedroom.

5. On or about August 8, 2019, agents with the FBI again interviewed **KOLLIE**, this time at his place of work. **KOLLIE** advised the FBI that he was concealed carry, which based upon my training and experience is an indication that he was carrying a firearm, and that he was claiming to have a permit to do so. The FBI observed a belt clip of what appeared to be an inside-the-waistband holster. **KOLLIE** informed the FBI that he and **BETTS** had done “hard

drugs,” marijuana, and acid together four to five times a week during 2014 to 2015. When asked how often he used drugs in the past year and a half, **KOLLIE** indicated that he smoked marijuana every day and had done so since he was fourteen. Agents asked **KOLLIE**: “So you never stopped,” or words to that effect. **KOLLIE** responded “that’s right,” or words to that effect. Based on my training and experience, and information from other law enforcement agents and officers, I am aware that marijuana is a controlled substance. The interviewing agents asked **KOLLIE** for consent to search his cellphone, but **KOLLIE** refused to give consent. Based on my training and experience, I know that individuals who use controlled substances, such as marijuana, use cellphones for purposes of buying controlled substances, communicating with their supplier, and storing contact information pertaining to their supplier.

6. Records obtained from a Dayton area Federal Firearm Licensed dealer included an ATF Form 4473, which based on my training and experience I know is required in order to complete the transaction of purchasing a firearm from a licensed dealer. The form pertained to the purchase by **KOLLIE** of a Century Arms Draco 7.62x39mm pistol with serial number PMD-11797-19. The form transferee/buyer was listed as **Ethan William KOLLIE** with the aforementioned address of the PREMISES, and a date of birth and social security number that is consistent with Ohio Bureau of Motor Vehicle records. The transfer of the firearm from the dealer to **KOLLIE** was completed on May 9, 2019.

7. Box 11e of the ATF Form 4473 states, “Are you an unlawful user of, or addicted to, marijuana or any depressant, stimulant, narcotic drug, or any other controlled substance? Warning: The use or possession of marijuana remains unlawful under Federal law regardless of

whether it has been legalized or decriminalized for medicinal or recreational purposes in the state where you reside.” **KOLLIE’s** Form 4473 was checked “No” in response to the question in box 11e.

TECHNICAL TERMS

8. Based on my training and experience, I use the following technical terms to convey the following meanings:

Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

9. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer’s hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

10. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is

typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

11. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the

sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks

and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer to research or purchase controlled substances or firearms, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may

contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

12. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the

warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

13. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

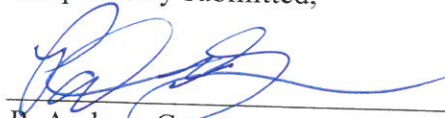
14. Because at least one other individual (a roommate) shares the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

15. Based on the foregoing, I believe there is probable cause to believe that crimes have been committed, namely, violations of 18 U.S.C. § 922(g)(3) (Possession of a firearm by an unlawful user of a controlled substance or by a person addicted to a controlled substance), 18 U.S.C. § 922(a)(6) (false statement regarding firearms), 18 U.S.C. § 924(a)(1)(A) (false statement regarding firearms); 18 U.S.C. § 1001 (false statement), and 21 U.S.C. § 844 (unlawful possession of a controlled substance), and that evidence, contraband, fruits of crime, and instrumentalities of crime will be found in the PREMISES.

16. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.


Respectfully submitted,



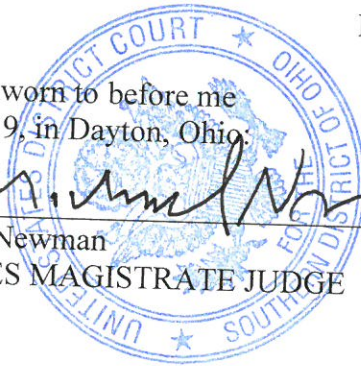
P. Andrew Gragan
Special Agent

Federal Bureau of Investigation

Subscribed and sworn to before me
on August 8, 2019, in Dayton, Ohio:



Hon. Michael J. Newman
UNITED STATES MAGISTRATE JUDGE



ATTACHMENT A

Property to be searched

The property to be searched is **1216 Cloverfield Avenue, Apartment D, Kettering, Ohio 45429**, further described as an apartment rented by **Ethan KOLLIE** and located at 1216 Cloverfield Avenue, Kettering, Ohio 45429, within a large multi-unit brick building with multiple front facing windows and blue shutters, as depicted in the photograph below. The apartment building has four tan in color pillars on the front of the building. The building has a concrete walkway leading from the sidewalk to a small concrete porch located near the front door. The front door is a large tan door with five small windows on each side. The apartment building's landscape consists of multiple small bushes running across the front of the building and two medium sized trees in the front yard. The building has a concrete driveway on the left side of the home leading to a large multiple car garage.



ATTACHMENT B

Property to be seized

1. All records relating to violations of:

- 18 U.S.C. § 922(g)(3)
- 18 U.S.C. § 922(a)(6)
- 18 U.S.C. § 924(a)(1)(A)
- 18 U.S.C. § 1001
- 21 U.S.C. § 844

involving **Ethan KOLLIE** and occurring after **2013**, including:

- a. any information related to the purchase, use, or possession of firearms;
- b. any information related to the purchase, use, or sale of controlled substances;
- c. any information related to the types, amounts, and prices of controlled substances or firearms purchased, used, or trafficked as well as dates, places, and amounts of specific transactions;
- d. any information related to sources of controlled substances or firearms (including names, addresses, phone numbers, or any other identifying information);
- e. any information recording **KOLLIE's** schedule or travel from 2013 to the present;
- f. all bank records, checks, credit card bills, account information, and other financial records.

- g. records of Internet Protocol addresses used;
 - h. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
- 2. Computers or storage media used as a means to commit the violations described above.
- 3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;

- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite"

web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

- m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law

enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.